TIME-STAMP SERVICE FOR THE NATIONAL INFORMATION NETWORK

This invention relates to computer technology and more particularly to a system for verifying the time at which a digital document is received by an authenticating agency together with verification of a digital signature supplied by the agency.

BACKGROUND OF THE INVENTION

The authenticity of signed paper documents is attested to by signing the document in the presence of a Notary Public. The Notary Public usually adds a permanent alteration to the document such as an impression of a seal together with the signature of the Notary and the date upon which the Notary witnessed the signature which is being authenticated.

There are many situations where it is important to prove that a digital document existed on a certain date and time in its current form. Sometimes it is also important to establish the authorship or at least the ownership of the digital document on that same day. Examples include the Disclosure of Inventions, ordinary commercial transactions such as Bills of Sale, or Payments of Invoices, Wills, and other contracts where time is a factor. While conventional Notaries Public can meet the need for ordinary documents written on paper, there is currently no generally available analogous service for documents that are in digital format. Examples of such documents include computer files generated by word processors or spreadsheet programs, and binary files such as compiled computer programs and digitized or scanned images such as are produced by scanners or facsimile machines. It is also needed to establish the authorship and date of creation for digital audio and digital video recordings.

U.S. Pat. Nos. 5,136,646; 5,136,647; and 5,373,561 disclose a system for time-stamping a digital document and catenating the certificate number with another document certified at some time prior to the current document. A subsequent document will refer to the certificate number of the current document. In that manner the time-stamp of the current document is placed between the time-stamping of two other documents received by the system. Such a system does not provide the exact time of receipt so therefore it attempts to show relative time by relating the time-stamp to previous and subsequent document receptions which may be owned by other parties.

U.S. Pat. No. 5,022,080 also relates to a system for time-stamping a received document. Once the time indication has been generated the received document and the generated time indication is encrypted to generate a combination of the two units of information.

U.S. Pat. Nos. 4,868,877; 5,001,752; 5,005,200 and 5,214,702 relate to a system in which a time-stamp is provided by a clock module operated by the authenticating party. The system is designed to certify a digital signature of the creating party through a hierarchy of nested certifications and signatures indicating the authority and responsibility of the agency granted to them by the individual whose signature is being certified.

It is desired to provide a simple system for proving that a digital document existed on a certain date and time in its current form. It is therefore an object of the invention to provide a system in which the accuracy of the time-stamp is unquestioned and in which there is no need to refer to previous or subsequent documents which may be owned by third parties.

It is a further object of the invention to provide a service in which a private key is used to add the signature of the authenticating agency through the use of a machine that is secure from an attack by network.

SUMMARY OF THE INVENTION

Briefly stated, this invention relates to a system for proving that a digital document existed on a certain date and time in its current form. The system applies a signed time-stamp to a document in digital format. When a document is received a time-stamp is applied utilizing the National Institute of Standards and Technology (NIST) cesium clock ensemble. The time of the receiving processor which may be connected into an electronic network is continuously adjusted to the cesium clock to keep it within a few milliseconds of that clock. After applying the time-stamp to the document, the document and the time-stamp are transferred to a second computer that is not connected to the Internet or any other electronic network for processing with a hashing algorithm to produce a numerical representation of the stamped document. A private key is utilized at the second processor for encrypting a digital signature of the authenticating agency and adding that encrypted digital signature to the hashed time-stamped document. The encrypted signed hashed time-stamped document is then returned to the network for sending it to the designated recipient.

The document can be authenticated by application of the hashing algorithm and the encrypted signature of the authenticating agency can be reproduced by application of a public key. If the document has been altered in any fashion, the authenticating process will fail. Thus, the accuracy of the original document, the time at which it was received by the authenticating agency, and the signature of the authenticating agency can be ascertained to prove the genuineness of the digital document.

The system can operate with any digital format including simple text files, binary files, scanned images, etc. The document can be encrypted or encoded by the sender. It can also be compressed by the sender so that the full text need not be revealed even to the authenticating agency. The system is designed to be computationally infeasible to alter the document or the time-stamp without invalidating the signature. It is also computationally infeasible to transfer the time-stamp or the signature to another document. The time-stamp is accurate to a few milliseconds and the accuracy is directly traceable to Universal Coordinated Time (UTC) with which it is synchronized. The system provides for public inspection of the time the computer used to time-stamp by making that time available over the network. The system can be accessed automatically via standard E-mail protocols or files can be transmitted to the authenticating agency manually using diskettes, tapes, or similar media. The signed document can be returned by mail or sent electronically or forwarded automatically to any number of third parties as requested by the sender. The signature can be verified by anyone using publicly available verify software and a standard personal computer or its equivalent. The system also supports optional authentication of the sender using an additional signature function. The system is designed to protect the signature keys by storing them on a machine that cannot be accessed over the network. If desired, a stand-alone machine not connected to a network can perform both time-stamping and signature functions.

The above mentioned and other features and objects of this invention and the manner of attaining them will become more apparent and the invention itself will best be under-